

Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of Claims:

1--38 (Canceled)

39. (new) A method for conducting private secure electronic commerce comprising the steps of:

providing first and second sequences of encryption key material wherein said first sequence is suited for decrypting a message that has been encrypted using said second sequence and the second sequence is suited for decrypting a message that has been encrypted using the first sequence, and the first sequence and second sequence each include an identical plurality of sequentially arranged session keys;

associating a value parameter with the first sequence;

providing the first sequence to an anonymous user in exchange for a payment;

providing encrypted data communication to said anonymous user utilizing said session keys of the first sequence until said value parameter is exhausted, by sub-steps comprising:

providing user-initiated connection to the anonymous user;

monitoring a connection time that is the time that the anonymous user is connected; and

requiring the anonymous user to utilize a new session key from the plurality of session keys of the first sequence after a predetermined connection time; and

adjusting the value parameter in response to utilization of the session keys of the first sequence such that when the plurality of session keys is exhausted, the value parameter is exhausted.

40. (new) A method for conducting private secure electronic commerce comprising the steps of:

providing first and second sequences of encryption key material wherein said first sequence is suited for decrypting a message that has been encrypted using said second sequence and the second sequence is suited for decrypting a message that has been encrypted using the first sequence, and the first sequence and second sequence each include an identical plurality of sequentially arranged session keys;

associating a value parameter with the first sequence;

providing the first sequence to an anonymous user in exchange for a payment;

providing encrypted data communication to said anonymous user utilizing said session keys of the first sequence until said value parameter is exhausted, by sub-steps comprising:

providing a user-initiated connection to the anonymous user;

recording a start time when said provided encrypted data communication first occurs; and

requiring said anonymous user to utilize a new session key from said plurality of session keys of said first sequence at predetermined intervals after said start time; and

adjusting the value parameter in response to utilization of the session keys of the first sequence such that when the plurality of session keys is exhausted, the value parameter is exhausted.

41. (new) A method for conducting private secure electronic commerce comprising the steps of:

providing first and second sequences of encryption key material wherein said first sequence is suited for decrypting a message that has been encrypted using said second sequence and the second sequence is suited for decrypting a message that has been encrypted using the first sequence, and the first sequence and second sequence each include an identical plurality of sequentially arranged session keys;

associating a value parameter with the first sequence;
providing the first sequence to an anonymous user in exchange for a payment;
providing encrypted data communication to said anonymous user utilizing
said session keys of the first sequence until said value parameter is exhausted, by sub-
steps comprising:

providing a user-initiated connection to the anonymous user;
monitoring the number of bytes of said communications; and
requiring said user to utilize a new session key from said
plurality of session keys of said first sequence after a predetermined
number of bytes of communication; and

adjusting the value parameter in response to utilization of the session keys of
the first sequence such that when the plurality of session keys is exhausted, the value
parameter is exhausted.

42. (new) A method for conducting private secure electronic commerce
comprising the steps of:

providing a first server that is an Internet service provider;
providing to an anonymous first user, in exchange for a payment, a first
sequence of encryption key material, an identifier associated with said first sequence,
connection instructions for connecting to said first server, and encryption instructions
for encrypting and decrypting data using the first sequence;

providing to the first server said identifier and a second sequence of
encryption key material suitable for decrypting data that is encrypted with the first
sequence and for encrypting data that can be decrypted with the first sequence;

establishing a first user account accessible to the first server, wherein said first
user account includes the identifier and a first user value parameter that is
proportional to said payment;

providing encrypted data communications in the form of anonymous Internet
access between said first user and the first server; and

adjusting said first user value parameter in response to said step of providing anonymous Internet access.

43. (new) The method as set forth in Claim 42, further including the steps of:
receiving a request for a service from said first user;
locating on the Internet a service provider that will provide said service;
establishing a service provider user account accessible to said first server including a service provider value parameter;
procuring said service for said first user from said service provider; and
adjusting said first user value parameter and said service provider value parameter in response to said step of procuring.

44. (new) A method for conducting private secure electronic commerce comprising the steps of:
providing a first server that is an anonymous email services provider;
providing to an anonymous first user, in exchange for a payment, a first sequence of encryption key material, an identifier associated with said first sequence, connection instructions for connecting to said first server, and encryption instructions for encrypting and decrypting data using the first sequence;
providing to the first server said identifier and a second sequence of encryption key material suitable for decrypting data that is encrypted with the first sequence and for encrypting data that can be decrypted with the first sequence;
establishing a first user account accessible to the first server, wherein said first user account includes the identifier and a first user value parameter that is proportional to said payment;
providing encrypted data communications in the form of anonymous email services to said first user; and
adjusting said first user value parameter in response to said step of providing anonymous email services to said first user.